NI 5205.1R3
Subgroup: Special Programs
Approved: 24 November 2003

NGA Instruction for Protection of Sensitive Compartmented Information

1. References.

a. Primary. NGA PD 5200R2, Policy Directive for Operational Security, 24 November 2003.

b. Secondary.

(1) DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, 1 May 2003.

(2) DCID 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI), 2 July 1998.

(3) DoD S-5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual, August 1998.

2. Purpose. Establish guidelines and responsibilities for the physical protection of sensitive compartmented information (SCI). This instruction supersedes NI 5205.1R2, same title, 1 November 2001.

3. Policy. NGA will develop and maintain the necessary procedures for the secure storage and use of SCI material maintained by the Agency. These procedures comply with all applicable regulations and directives. NGA personnel and contractors who are indoctrinated for access to SCI are individually and personally responsible for providing proper protection for that SCI material that is in their custody and control.

4. Applicability and Scope. This instruction applies to all NGA employees, military personnel, and contractor personnel. As a combined DoD and IC organization, NGA must properly control, protect, and dispose of all SCI that is generated or acquired. This instruction addresses the operational security aspects of managing the NGA SCI program.

5. Definitions.

a. Sensitive compartmented information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes that must be handled within formal access control systems established by the Director of Central Intelligence.

b. Sensitive compartmented information facility (SCIF). An accredited area, room, group of rooms, buildings, or installations where SCI is stored, used, discussed, or processed. SCIF procedural and physical measures prevent the free

access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF.

c. Special security officer (SSO). The person responsible for the security management, operation, implementation, use, and dissemination of all types of SCI material within their organization or site.

6. Responsibilities.

a. Security and Installation Operations Directorate, Security Office (SIS).

(1) Negotiates and administers the necessary resources to ensure proper protection and control for SCI material in NGA custody.

(2) Appoints SSOs within each site security work team to oversee protection of SCI material at that site.

(3) Conducts required security education and training to ensure that all Agency personnel are familiar with procedures necessary for the protection of SCI material.

b. NGA organizations, with SSO oversight, implement the procedures specified in this instruction and other applicable regulations, directives, and manuals to ensure protection of SCI materials in their custody.

7. Procedures.

a. SIS personnel provide SCI advice and assistance to Agency personnel and maintain all applicable guidance to adequately discharge NGA SCI duties.

b. All SCI materials in NGA custody are properly accounted for, controlled, transmitted, transported, packaged, and safeguarded in accordance with guidelines established by SIS and those external organizations with cognizance over the SCI program.

c. SCI materials are disseminated only to those individuals who have an established need-to-know and the appropriate accesses.

d. Requests for access to SCI materials in specific compartments, prepared in writing and signed by the supervisor, are submitted to the personnel security program manager, Personnel Security Division (SISP). Requests are reviewed by SISP and forwarded to the appropriate compartment program manager for consideration.

e. All NGA employees with access to SCI.

(1) Report to the local site security team any information that could reflect on the trustworthiness of an individual who has access to SCI material.

(2) Report possible security violations or compromises to the site security team.

(3) Report any unauthorized disclosure or exposure of SCI.

(4) Take immediate action to protect SCI found in a non-secure environment until the documents can be restored to SCI control.

(5) Refrain from putting such material on the sensitive-but-unclassified (SBU) or any other non-SCI computer network under any circumstances.